هل مشروعك التجاري مُعرَّضٌ لـ الهجوم السيبراني؟

ما الهجوم السيبراني ؟

هو نوع من المناورة الهجومية التي تستهدف نظام الكمبيوتر أو شبكة الإنترنت، مما يتسبب في فقدان البيانات والمعلومات وإلحاق ضرر كبير بالشركات والأفراد عبر فقدانهم لبياناتهم الشخصية.

لذا من المهم للجميع اتخاذ الإجراءات وتأمين البيانات من الهجوم السيبراني.

أرقام حقيقية

43% من الهجمات السيبرانية تستهدف المشاريع الناشئة

14 ثانية تحدث هجمة باستخدام فيروس الفدية

91% من الهجمات تحدث عبر رسائل البريد الإلكتروني غير المرغوب بها

أنواع شائعة من الهجمات السيبرانية

هجوم الاحتيال الإلكتروني

يتم تنفيذ هذا النوع من الهجوم عبر البريد الإلكتروني للحصول على معلومات شخصية، عبر إرسال رسائل غير مرغوب بها من مصادر غير موثوقة.

هجوم الفيروسات

تعد الأنشطة الضارة مثل إدخال الفيروسات والملفات المصابة وفيروسات الفدية وغيرها في نظام الكمبيوتر أو الجهاز المحمول بشكل عام شكلًا من أشكال هجوم البرمجيات الخبيثة.

هجوم عبر التنزيل

يتم تنفيذ هذا النوع من الهجوم من قبل المخترقين على مواقع الويب غير الآمنة حيث يزرعون الڤيروسات في شفرة الموقع الإلكتروني ثم يقومون بمهاجمة نظام زوار الموقع

هجوم كلمة المرور

يتم تنفيذه بنية اختراق نظام الكمبيوتر أو شبكة الانترنت بعدة طرق منها هجوم القوة الغاشمة وهجوم القاموس والهجوم براصد لوحة المفاتيح

كيف تتجنب الهجمات السيبرانية؟

قم بتثبيت برنامج مكافحة الڤيروسات على جهازك

يكشف برنامج مكافحة الڤيروسات البرمجيات الضارة في نظامك ويقضي عليها، وبالتالي يحافظ على بياناتك ومعلوماتك آمنة، لذا تأكد من تثبيت مضاد ڤيروسات موثوق به في جهازك

استخدم كلمات مرور قوية وغيِّرها بشكل دوري

يمكن أن يساعدك استخدام كلمة مرور قوية وغير سهلة الاختراق في تأمين معلوماتك وبياناتك. قم بتعيين كلمة مرور مختلفة في مختلف التطبيقات التي تستخدمها وغيِّرها بصورة دورية وذلك كإجراء احترازي

كن حذرًا أثناء تثبيت البرنامج

قد تحتوي البرامج المثبتة من مصادر غير موثوقة على برمجيات ضارة مرتبطة بها مما قد يؤدي إلى فقدان البيانات أو حدوث خلل في النظام، لذا يفضل تثبيت البرامج الموثوق بها وتجنب تحميل البرامج المجانية عبر الإنترنت

احرص دائمًا على تحديث نظامك

تحتوي أحدث إصدارات البرامج وأنظمة التشغيل على تصحيحات الأمان المهمة للتعامل مع البرمجيات الضارة، لذا يجب عليك التأكد من تحديث جميع البرامج ونظام التشغيل الذي تستخدمه إلى أحدث إصداراتها

كن حذراً من رسائل البريد الإلكتروني غير المرغوب بها

تعدُّ رسائل البريد الإلكتروني أو الروابط المزيّفة أسهل طريقة ليهاجم بها الڤيروس نظامك، لذلك يجب ألا تفتح أي روابط عشوائية تصلك على البريد الإلكتروني من مصادر غير معروفة، كما يمكنك اختيار خدمات أمان البريد الإلكتروني التي تساعد في حماية نظامك والكشف عن الرسائل غير المرغوبة.

قم بإجراء النسخ الاحتياطي للبيانات والمعلومات الخاصة بك بشكل دوريّ

يساعد النسخ الاحتياطي للبيانات على استعادتها والحفاظ عليها آمنة في حالة الهجمات السيبرانية. لذلك، يجب عليك دائمًا الاحتفاظ بنسخة احتياطية من جميع بياناتك ومعلوماتك بانتظام على جهاز مختلف.

اختر مزود خدمات سحابية موثوق به

يعد تخزين البيانات على السحابة واحدة من أفضل الطرق لإبقائها آمنة لأنها توفر العديد من ميزات الأمان والنسخ الاحتياطي، لذلك يمكنك اختيار مزود خدمات سحابية موثوق به وفقًا لاحتياجات تخزين البيانات الخاصة بك.

ترجمة: هدى القطيطية
تدقيق: مريم الغافرية
المصدر: acecloudhosting.com

نادي كلمة
Word-Club.net
@Word_Club